39651BLU.TOO HB-0301 26/3/01

FIELD OF THE INVENTION

[0001] The present invention relates to authentication in computer systems generally.

BACKGROUND OF THE INVENTION

[0002] The following publications are believed to represent the state of the art relevant to the present invention:

"Bluetooth Security Architecture, Version 1.0" by Thomas Muller, July 15th 1999;

"Bluetooth specifications core, Version 1.0b", Dec 1st 1999;

"Bluetooth specifications profile, Version 1.0b", Dec 1st 1999;

"First Access and Bluetooth Announce Technological Collaboration", February 21, 2000;

"CeBit bluetooth™ pavilion to showcase Ensure's patented XyLoc wireless pc security", February 24, 2000;

U.S. Patent No. 6070240.

SUMMARY OF THE INVENTION

[0003] There is thus provided in accordance with a preferred embodiment of the present invention a device capable of communicating with an authenticator at least partially using a Bluetooth communication protocol. The device includes at least one authentication functionality, at least part of at least one of which operates to communicate authentication information via the Bluetooth communication protocol.

[0004] There is provided in accordance with another preferred embodiment of the present invention a device capable of communicating with an authenticator. The device includes at least one authentication functionality at least part of at least one of which forms part of the Bluetooth communication protocol.

[0005] There is provided in accordance with a preferred embodiment of the present invention a device capable of communicating with an authenticator at least partially using a Bluetooth communication protocol. The device includes at least one

authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

[0006] There is also provided in accordance with a preferred embodiment of the present invention a system including a communication network, at least one authenticator and at least one device capable of communicating with the authenticator through the communication network, via a Bluetooth communication protocol. The device includes at least one authentication functionality, at least part of at least one of which is operative to communicate authentication information via the Bluetooth communication protocol to the at least one authenticator.

[0007] There is also provided in accordance with yet another preferred embodiment of the present invention a system including a communication network, at least one authenticator and at least one device capable of communicating communicating with the authenticator through the communication network. The device includes at least one authentication functionality, at least part of at least one of which forms part of the Bluetooth communication protocol.

[0008] There is also provided in accordance with a preferred embodiment of the present invention a system including a communication network, at least one authenticator and at least one device capable of communicating with the authenticator through the communication network, via a Bluetooth communication protocol. The device includes at least one authentication functionality at least part of at least one of which employs a Bluetooth communication protocol

[0009] There is provided in accordance with another preferred embodiment of the present invention a system including at least one authenticator and at least one device capable of communicating with the authenticator via a Bluetooth communication protocol. The device includes at least one authentication functionality, at least part of at least one of which is operative to communicate authentication information via the Bluetooth communication protocol to the authenticator.

[0010] There is further provided in accordance with yet another preferred embodiment of the present invention a system including at least one authenticator and at least one device capable of communicating with the authenticator. The device includes at least one authentication functionality, at least part of at least one of which forms part of the Bluetooth communication protocol.

[0011] There is further provided in accordance with another preferred embodiment of the present invention a system including at least one authenticator and at least one device capable of communicating with the authenticator via a Bluetooth communication protocol. The device includes at least one authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

[0012] There is provided in accordance with a preferred embodiment of the present invention a system including at least one device and at least one second device. Said system includes at least one multi-tier authentication functionality, at least part of at least one of which operates to communicate authentication information via the Bluetooth communication protocol to at least one authenticator.

[0013] There is provided in accordance with a preferred embodiment of the present invention a system including at least one device and at least one second device. Said system includes at least one multi-tier authentication functionality, at least part of at least one of which forms part of the Bluetooth communication protocol.

[0014] There is provided in accordance with a preferred embodiment of the present invention a system including at least one device and at least one second device. Said system includes at least one multi-tier authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

[0015] There is further provided in accordance with yet another preferred embodiment of the present invention a method for authenticating with an authenticator. The method includes at least one authentication functionality, at least part of at least one of which is operative to communicate authentication information via the Bluetooth communication protocol.

[0016] There is further provided in accordance with yet another preferred embodiment of the present invention a method for authenticating with an authenticator. The method includes at least one authentication functionality, at least part of at least one of which forms part of the Bluetooth communication protocol.

[0017] There is further provided in accordance with yet another preferred embodiment of the present invention a method for authenticating with an authenticator. The method includes at least one authentication functionality at least part of at least one of which employs a Bluetooth communication protocol.

[0018] Further in accordance with a preferred embodiment of the present

invention the device is effective in identifying at least one of the device, another device, a user of the device and the user of the other device, to at least one authenticator coupled to the communication network.

[0019] Additionally in accordance with a preferred embodiment of the present invention the device is a dedicated authentication device.

[0020] Further in accordance with a preferred embodiment of the present invention the device includes substantial non-authentication functionality.

[0021] Preferably, the device includes a telephone, a PDA, a computer, an electronic wallet and a wireless smart card.

[0022] Further in accordance with a preferred embodiment of the present invention the authentication functionality is selected from the following authentication functionalities: a cryptographic authentication functionality, a password based authentication functionality, a smartcard based authentication functionality, a token based authentication functionality and a biometric based authentication functionality.

[0023] Additionaly in accordance with a preferred embodiment of the present invention the authentication functionality forms part of the Bluetooth communication protocol.

[0024] Additionaly in accordance with a preferred embodiment of the present invention the authentication functionality includes at least a plurality of the following authentication functionalities: a cryptographic authentication functionality, a password based authentication functionality, a smartcard based authentication functionality, a token based authentication functionality and a biometric based authentication functionality.

[0025] Additionaly in accordance with a preferred embodiment of the present invention, the authentication functionality includes plural authentication functionalities.

[0026] Preferably, the device includes substantial non-authentication functionality wherein the authentication functionality includes plural authentication functionalities.

[0027] Preferably, the device is a dedicated authentication device and the authentication functionality includes plural authentication functionalities.

BRIEF DESCRIPTION OF THE DRAWINGS

[0028] The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified pictorial illustration of a system and methodology for authentication and communication with a communication network employing a Bluetooth communication protocol in accordance with a preferred embodiment of the present invention;

Fig. 2 is a simplified pictorial illustration of a system and methodology for authentication communication with computer employing a Bluetooth communication protocol in accordance with another preferred embodiment of the present invention;

Fig. 3 is a simplified pictorial illustration of a system and methodology for multi-tier authentication and communication with a communication network employing a Bluetooth communication protocol in accordance with a preferred embodiment of the present invention;

Fig. 4 is a simplified pictorial illustration of a system and methodology for authentication and communication, using a Bluetooth communication protocol, with a communication network in accordance with yet another preferred embodiment of the present invention;

Fig. 5 is a simplified pictorial illustration of a system and methodology for authentication and communication, using a Bluetooth communication protocol, with a computer in accordance with yet another preferred embodiment of the present invention;

Fig. 6 is a simplified pictorial illustration of a system and methodology for multi-tier authentication and communication, using a Bluetooth communication protocol, with a communication network in accordance with yet another preferred embodiment of the present invention;

Fig. 7 is a simplified pictorial illustration of a system and methodology for authentication, using a Bluetooth communication protocol, and communication with a communication network in accordance with yet another preferred embodiment of the present invention;

Fig. 8 is a simplified pictorial illustration of a system and methodology for authentication, using a Bluetooth communication protocol, and communication with a computer in accordance with yet another preferred embodiment of the present invention;

Fig. 9 is a simplified pictorial illustration of a system and methodology for multi-tier authentication, using a Bluetooth communication protocol, and communication with a communication network in accordance with yet another preferred embodiment of the present invention;

Figs. 10A, 10B, 10C, 10D and 10E are simplified pictorial illustrations of single authentication functionalities appropriate for five different types of authentication devices;

Figs. 11A, 11B, 11C, 11D, 11E and 11F are simplified pictorial illustrations of combinations of authentication functionalities appropriate for six different combinations of different types of authentication devices;

Figs. 12A, 12B and 12C are simplified pictorial illustrations of combinations of authentication functionalities appropriate for three different multi-tier combinations of different types of authentication devices;

Figs. 13A, 13B, 13C, 13D and 13E are simplified flow charts of single authentication functionalities appropriate for five different types of authentication devices and correspond to Figs. 10A - 10E;

Figs. 14A, 14B, 14C, 14D, 14E and 14F are simplified flow charts of combinations of authentication functionalities appropriate for six different combinations of different types of authentication devices and correspond to Figs. 11A - 11F;

Figs. 15A, 15B, 15C, 15D and 15E are simplified flow charts of methods for obtaining authentication information for five different types of authentication devices;

Figs. 16A, 16B and 16C are simplified flow charts of various multi-tier and non multi-tier authentication methods using different communication modes between an authenticating device and an authenticator; and

Figs. 17A, 17B and 17C are simplified flow charts of various multi-tier and non multi-tier authentication methods employing different combinations of authentication devices.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0029] Reference is now made to Fig. 1, which is a simplified pictorial illustration of a system and methodology for communication with a communication network employing a Bluetooth communication protocol in accordance with a preferred embodiment of the present invention. As seen in Fig. 1, there is provided an authentication system 100 communicating with a communication network, such as the Internet, herein designated by reference numeral 102 or with an intranet.

[0030] For the purposes of the present application "authentication" is to be understood broadly as referring to any process or functionality for providing authorization, access control, permission or approval. The phase "authentication information" is to be understood as any information which is employed for the purpose of authentication.

[0031] In accordance with a preferred embodiment of the present invention, the authentication system is effective to identify at least one of at least one device, such as a PC 104, a telephone 106 and a wireless smart card 108, and at least one user thereof to at least one authenticator, represented by a lock symbol and designated by reference numeral 110, coupled to the communication network 102 and arranged to provide an indication of such authentication to other computers, such as those designated by reference numeral 112, such as web servers, database servers and application servers.

[0032] In accordance with one embodiment of the present invention, at least one device, such as PC 104, communicates with the communication network 102 using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral 114. PC 104 typically includes multiple authentication functionalities, symbolized by multiple keys. As seen in Fig. 1, one of the authentication functionalities is a password authentication functionality, designated by reference numeral 116. Additionally or alternatively a cryptographic authentication functionality may also be provided, such as by means of a USB token 118 which may be associated with the PC 104.

[0033] Additionally in accordance with an embodiment of the present invention, telephone 106 communicates with the communication network 102 in any suitable manner and may or may not employ a Bluetooth communication protocol for

communication. In this example, authentication may employ functionality, at least part of which forms part of the Bluetooth communication protocol, as symbolized by a tooth overlaid with a key, collectively designated by reference numeral 120.

[0034] In a further example, a dedicated authentication device, such as the wireless smart card 108 providing access control, communicates with the communication network 102 for authenticating a user thereof and includes cryptographic authentication functionality, symbolized by a key and here specifically designated by reference numeral 122, which communicates with authenticator 110 using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral 124.

[0035] It is appreciated that authentication may be provided in the embodiment of Fig. 1 by any one or more of the authentication functionalities described hereinabove. Thus authentication may require both Bluetooth authentication functionality and password authentication functionality, provided by telephone 106 and computer 104 respectively.

[0036] Reference is now made to Fig. 2, which is a simplified pictorial illustration of a system and methodology for authentication employing a Bluetooth communication protocol in accordance with a preferred embodiment of the present invention. As seen in Fig. 2, there is provided an authentication system 200 wherein one or more authentication devices communicate with a computer 202, which itself includes an authenticator 210.

[0037] In accordance with a preferred embodiment of the present invention, the authentication system 200 is effective to identify at least one of at least one authentication device and at least one user thereof to at least one authenticator

[0038] The authentication devices typically include a personal digital assistant 212, a smart card 214 and an electronic wallet 216. Personal digital assistant 212 communicates with the computer 202 using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral 218 and typically employs a biometric authentication functionality, such as a touch screen fingerprint sensor based authentication functionality, indicated by reference numeral 220.

[0039] Smart card 214 may be a wireless smart card which may employ an

authentication functionality at least part of which may form part of the Bluetooth communication protocol, as symbolized by a tooth overlaid with a key, collectively designated by reference numeral 222.

[0040] Electronic wallet 216 communicates with the computer 202 using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral 224. Electronic wallet 216 may employ cryptographic authentication functionality, symbolized by a key and here specifically designated by reference numeral 226.

[0041] It is appreciated that authentication may be provided in the embodiment of Fig. 2 by any one or more of the authentication devices described hereinabove. Thus a user may be required to provide both biometric inputs and cryptographic inputs, as by using the personal digital assistant 212 and the electronic wallet 216 respectively.

[0042] Reference is now made to Fig. 3, which is a simplified pictorial illustration of a system and methodology for multi-tier authentication and communication with a communication network employing a Bluetooth communication protocol in accordance with a preferred embodiment of the present invention.

[0043] As seen in Fig. 3, there is provided an authentication system 300 communicating with a communication network, such as the Internet, herein designated by reference numeral 302 or with an intranet. System 300 is effective to identify at least one of at least one device, such as a suitably equipped PC 304, a personal digital assistant 306 and an electronic wallet 308, and at least one user thereof to at least one authenticator, represented by a lock symbol and designated by reference numeral 310, coupled to the communication network 302 and arranged to provide an indication of such authentication to other computers, such as those designated by reference numeral 312, such as web servers, database servers and application servers.

[0044] In accordance with a preferred embodiment of the present invention, the authentication system provides multi-tier authentication in that one or more devices, such as personal digital assistant 306, electronic wallet 308 and PC 304, which communicate via Bluetooth, are employed in order to authenticate one or more devices or a user thereof to authenticator 310.

[0045] In accordance with one embodiment of the present invention, at least one device, such as PC 304, communicates with the communication network 302 using a

Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral 314. The at least one device, such as PC 304 may authenticate itself and/or another device or a user to authenticator 310 by means of an authentication functionality at least part of which forms part of the Bluetooth communication protocol.

[0046] Additionally or alternatively, the at least one device, such as PC 304 may authenticate itself and/or another device or a user to authenticator 310 by means of a cryptographic authentication functionality, provided such as by means of a key diskette 316, which may be associated with the at least one device.

[0047] The personal digital assistant 306 may communicate with the PC 304 using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral 318. The personal digital assistant 306 may authenticate itself and/or another device or a user to authenticator 310 by means of a password authentication functionality.

[0048] The electronic wallet 308 may employ an authentication functionality at least part of which may form part of the Bluetooth communication protocol, as symbolized by a tooth overlaid with a key, collectively designated by reference numeral 320 and may or may not employ a Bluetooth communication protocol for communication.

[0049] The multiple-tier authentication functionality of Fig. 3 may operate in one or more of typically four modes:

The PC 304 may be used merely to communicate to network 302 authentication information sent by personal digital assistant 306.

The PC 304 may be used as an authentication proxy when suitably enabled by receipt of authentication information from the personal digital assistant 306.

The PC 304 may be used as an authentication proxy when suitably enabled by receipt of Bluetooth authentication from the electronic wallet 308.

The personal digital assistant 306 may be used to enable the PC 304 to authenticate itself or a user thereof to the authenticator 310.

The electronic wallet 308 may be used to enable the PC 304 to authenticate itself or a user thereof to the authenticator 310.

[0050] It is appreciated that authentication may be provided in the embodiment of Fig. 3 by any one or more of the authentication devices described hereinabove. Thus

a user may be required to provide both password inputs and cryptographic inputs, as by using the personal digital assistant 306 and the key diskette 316 respectively.

[0051] Reference is now made to Fig. 4, which is a simplified pictorial illustration of a system and methodology for communication, using a Bluetooth communication protocol, and authentication with a communication network in accordance with yet another preferred embodiment of the present invention. As seen in Fig. 4, there is provided an authentication system 400 communicating with a communication network, such as the Internet, herein designated by reference numeral 402 or with an intranet.

[0052] Five different types of devices are shown here in Bluetooth communication via computer network 402 with an authenticator 410: a wireless smart card 412, an electronic wallet 414, a telephone 416, a personal digital assistant 418 and a PC 420. It is appreciated that any suitable device may alternatively or additionally communicate via computer network 402 with authenticator 410.

[0053] In accordance with a preferred embodiment of the present invention, the authentication system is effective to identify at least one device or a user thereof to at least one authenticator 410, represented by a lock symbol, coupled to the communication network 402 and arranged to provide an indication of such authentication to other computers, such as those designated by reference numeral 422, such as web servers, database servers and application servers.

[0054] In accordance with one embodiment of the present invention, at least one device, such as PC 420, communicates with the communication network 402 using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral 424. PC 420 typically includes multiple authentication functionalities, symbolized by multiple keys associated respectively with a smart card 426, a key diskette 428 and a USB token 430. As symbolized by key 432, the PC 420 may also provide additional authentication functionalities.

[0055] Additional devices, such as wireless smart card 412, electronic wallet 414, telephone 416 and personal digital assistant 418 each also communicate with the communication network 402 using a Bluetooth communication protocol, as symbolized respectively by a tooth and designated by respective reference numerals 442, 444, 446 and 448. Each such additional device may include a single authentication functionality

or multiple authentication functionalities.

[0056] It is appreciated that authentication may be provided in the embodiment of Fig. 4 by any one or more of the authentication devices and/or functionalities described hereinabove.

[0057] Reference is now made to Fig. 5, which is a simplified pictorial illustration of a system and methodology for communication, using a Bluetooth communication protocol, and authentication in accordance with yet another preferred embodiment of the present invention. As seen in Fig. 5, there is provided an authentication system 500 wherein one or more authentication devices communicate with a computer 502, which itself includes an authenticator 510.

[0058] Four different types of devices are shown here in Bluetooth communication with computer 502 which itself includes authenticator 510: a wireless smart card 512, an electronic wallet 514, a telephone 516 and a personal digital assistant 518. It is appreciated that any suitable device may alternatively or additionally communicate with computer 502, which itself includes an authenticator 510.

[0059] In accordance with a preferred embodiment of the present invention, the authentication system is effective to identify at least one device or a user thereof to at least one authenticator 510, represented by a lock symbol.

[0060] In accordance with one embodiment of the present invention, at least one device, such as personal digital assistant 518 communicates with the computer 502, which itself includes an authenticator 510, using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral 524. Personal digital assistant 518 may include a single authentication functionality or multiple authentication functionalities.

[0061] Additional devices, such as wireless smart card 512, electronic wallet 514 and telephone 516 each also communicate with the computer 502 using a Bluetooth communication protocol, as symbolized respectively by a tooth and designated by respective reference numerals 542, 544 and 546. Each such additional device may include a single authentication functionality or multiple authentication functionalities.

[0062] It is appreciated that authentication may be provided in the embodiment of Fig. 5 by any one or more of the authentication devices and/or functionalities described hereinabove.

[0063] Reference is now made to Fig. 6, which is a simplified pictorial illustration of a system and methodology for communication, using a Bluetooth communication protocol, and authentication with a communication network in accordance with yet another preferred embodiment of the present invention. As seen in Fig. 6, there is provided an authentication system 600 communicating with a communication network, such as the Internet, herein designated by reference numeral 602 or with an intranet.

[0064] Four different types of authentication devices are shown here in Bluetooth communication with a computer 604: a wireless smart card 612, an electronic wallet 614, a telephone 616 and a personal digital assistant 618. It is appreciated that any suitable device may alternatively or additionally communicate with computer 604, which in turn communicates via network 602 with at least one authenticator 620, represented by a lock symbol, coupled to the communication network 602 and arranged to provide an indication of such authentication to other computers, such as those designated by reference numeral 622, such as web servers, database servers and application servers.

[0065] In accordance with a preferred embodiment of the present invention, the authentication system 600 is effective to identify at least one device or a user thereof to at least one authenticator 620.

[0066] In accordance with a preferred embodiment of the present invention, the authentication system provides multi-tier authentication.

[0067] In accordance with one embodiment of the present invention, at least one authentication device, such as personal digital assistant 618 communicates with the computer 604, using a Bluetooth communication protocol, symbolized by a tooth and specifically designated by reference numeral 624. Computer 604 in turn communicates with authenticator 620 via communication network 602. Personal digital assistant 618 may include a single authentication functionality or multiple authentication functionalities.

[0068] Additional authentication devices, such as wireless smart card 612, electronic wallet 614 and telephone 616 each also communicate with the computer 604 using a Bluetooth communication protocol, as symbolized respectively by a tooth and designated by respective reference numerals 642, 644 and 646. Each such additional

device may include a single authentication functionality or multiple authentication functionalities.

[0069] The multiple-tier authentication functionality of Fig. 6 may operate in one or more of typically three modes:

The computer 604 may be used merely to communicate to network 602 authentication information sent by any of the above-described authentication devices.

The computer 604 may be used as an authentication proxy when suitably enabled by receipt of authentication information from the any of the above-described authentication devices.

Any of the above-described authentication devices may be used to enable the computer 604 to authenticate itself or a user thereof to the authenticator 620.

[0070] It is appreciated that authentication may be provided in the embodiment of Fig. 6 by any one or more of the authentication devices and/or functionalities described hereinabove.

[0071] Reference is now made to Fig. 7, which is a simplified pictorial illustration of a system and methodology for authentication, using a Bluetooth communication protocol, and communication with a communication network in accordance with yet another preferred embodiment of the present invention. As seen in Fig. 7, there is provided an authentication system 700 communicating with a communication network, such as the Internet, herein designated by reference numeral 702 or with an intranet.

[0072] Five different types of devices are shown here in communication via computer network 702 with an authenticator 710: a wireless smart card 712, an electronic wallet 714, a telephone 716, a personal digital assistant 718 and a PC 720. It is appreciated that any suitable device may alternatively or additionally communicate via computer network 702 with authenticator 710.

[0073] In accordance with a preferred embodiment of the present invention, the authentication system is effective to identify at least one device or a user thereof to at least one authenticator 710, represented by a lock symbol, coupled to the communication network 702 and arranged to provide an indication of such authentication to other computers, such as those designated by reference numeral 722, such as web servers, database servers and application servers.

[0074] In accordance with one embodiment of the present invention, at least one device, such as PC 720, communicates with the communication network 702. PC 720 may include one or more authentication functionalities, at least part of at least one of them forming part of a Bluetooth communication protocol, as symbolized by a tooth overlaid by a key and designated by reference numeral 724.

[0075] Additional devices, such as wireless smart card 712, electronic wallet 714, telephone 716 and personal digital assistant 718 each also provide authentication via the communication network 702 using an authentication functionality, at least part of which forms part of a Bluetooth communication protocol, as symbolized respectively by a tooth overlaid by a key and designated by respective reference numerals 742, 744, 746 and 748.

[0076] It is appreciated that authentication may be provided in the embodiment of Fig. 7 by any one or more of the authentication devices and/or functionalities described hereinabove.

[0077] Reference is now made to Fig. 8, which is a simplified pictorial illustration of a system and methodology for authenticating using an authentication functionality, at least part of which forms at least part of a Bluetooth communication protocol in accordance with yet another preferred embodiment of the present invention. As seen in Fig. 8, there is provided an authentication system 800 wherein one or more authentication devices communicate with a computer 802, which itself includes an authenticator 810.

[0078] Four different types of devices are shown here in communication with computer 802 which itself includes authenticator 810: a wireless smart card 812, an electronic wallet 814, a telephone 816 and a personal digital assistant 818. It is appreciated that any suitable device may alternatively or additionally communicate with computer 802, which itself includes an authenticator 810.

[0079] In accordance with a preferred embodiment of the present invention, the authentication system is effective to identify at least one device or a user thereof to at least one authenticator 810, represented by a lock symbol.

[0080] In accordance with one embodiment of the present invention, at least one device, such as personal digital assistant 818 communicates with the computer 802, which itself includes an authenticator 810, and authenticates to the authenticator 810

employing an authentication functionality, at least part of which forms part of a Bluetooth communication protocol, symbolized by a tooth overlaid by a key and specifically designated by reference numeral 824.

[0081] Additional devices, such as wireless smart card 812, electronic wallet 814 and telephone 816 each may communicate with the computer 802 and may authenticate using an authentication functionality at least part of which forms part of a Bluetooth communication protocol, as symbolized respectively by a tooth overlaid with a key and designated by respective reference numerals 842, 844 and 846.

[0082] It is appreciated that authentication may be provided in the embodiment of Fig. 8 by any one or more of the authentication devices and/or functionalities described hereinabove.

[0083] Reference is now made to Fig. 9, which is a simplified pictorial illustration of a system and methodology for authentication, using an authentication functionality, at least part of which forms at least part of a Bluetooth communication protocol, via a communication network in accordance with yet another preferred embodiment of the present invention. As seen in Fig. 9, there is provided an authentication system 900 communicating with a communication network, such as the Internet, herein designated by reference numeral 902 or with an intranet.

[0084] Four different types of authentication devices are shown here in communication with a computer 904: a wireless smart card 912, an electronic wallet 914, a telephone 916 and a personal digital assistant 918. It is appreciated that any suitable device may alternatively or additionally communicate with computer 904, which in turn communicates via network 902 with at least one authenticator 920, represented by a lock symbol, coupled to the communication network 902 and arranged to provide an indication of such authentication to other computers, such as those designated by reference numeral 922, such as web servers, database servers and application servers.

[0085] In accordance with a preferred embodiment of the present invention, the authentication system 900 is effective to identify at least one device or a user thereof to at least one authenticator 920.

[0086] In accordance with a preferred embodiment of the present invention, the authentication system provides multi-tier authentication.

[0087] In accordance with one embodiment of the present invention, at least one authentication device, such as personal digital assistant 918, communicates with the computer 904 and provides authentication using an authentication functionality, at least part of which forms at least part of a Bluetooth communication protocol, symbolized by a tooth overlaid with a key and specifically designated by reference numeral 924. Computer 904 in turn communicates with authenticator 920 via communication network 902.

[0088] Additional authentication devices, such as wireless smart card 912, electronic wallet 914 and telephone 916 each may provide authentication using an authentication functionality, at least part of which forms at least part of a Bluetooth communication protocol, as symbolized respectively by a tooth overlaid by a key and designated by respective reference numerals 942, 944 and 946.

[0089] The multiple-tier authentication functionality of Fig. 9 may operate in one or more of typically three modes:

The computer 904 may be used merely to communicate to network 902 authentication information sent by any of the above-described authentication devices.

The computer 904 may be used as an authentication proxy when suitably enabled by receipt of authentication information from the any of the above-described authentication devices.

Any of the above-described authentication devices may be used to enable the computer 904 to authenticate itself or a user thereof to the authenticator 920.

[0090] It is appreciated that authentication may be provided in the embodiment of Fig. 9 by any one or more of the authentication devices and/or functionalities described hereinabove.

[0091] Reference is now made to Figs. 10A, 10B, 10C, 10D and 10E which are simplified pictorial illustrations of single authentication functionalities appropriate for five different types of authentication devices and to Figs. 13A, 13B, 13C, 13D and 13E, which are simplified flow charts of single authentication functionalities appropriate for five different types of authentication devices and correspond to Figs. 10A - 10E.

[0092] Fig. 10A illustrates five different authentication functionalities for a personal digital assistant. As seen in Fig. 10A, a personal digital assistant with associated camera, here designated by reference numeral 1000, provides authentication

using facial recognition and communicates with an authenticator 1001, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0093] Additionally or alternatively, a personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner here designated by reference numeral 1002, provides authentication using fingerprint recognition and communicates with authenticator 1001, typically at least partially using a Bluetooth communication protocol.

[0094] Additionally or alternatively, a personal digital assistant, which may be of conventional design and construction, here designated by reference numeral 1004, provides password based authentication and communicates with authenticator 1001, typically at least partially using a Bluetooth communication protocol.

[0095] Additionally or alternatively, a personal digital assistant, which may be of conventional design and construction, here designated by reference numeral 1006, provides cryptographic authentication and communicates with authenticator 1001, typically at least partially using a Bluetooth communication protocol.

[0096] Additionally or alternatively, a personal digital assistant, which may be of conventional design and construction, here designated by reference numeral 1008, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0097] It is appreciated that authentication may be provided in the embodiment of Fig. 10A by any one or more of the authentication devices and/or functionalities described hereinabove.

[0098] Reference is now made to Fig. 13A, which illustrates the authentication functionalities shown in Fig. 10A. As seen in Fig. 13A, a user who requests access to a resource protected by an authenticator may employ a personal digital assistant (PDA) to negotiate an authentication functionality. Depending on the facilities available in or in association with the personal digital assistant, one of the following authentication functionalities may be selected:

biometric utilizing fingerprint recognition;

biometric utilizing facial recognition;

password based;

cryptographic key based; and

Bluetooth based.

[0099] If the biometric authentication functionality utilizing fingerprint recognition is selected, the personal digital assistant captures the user's fingerprint data.

[0100] If the biometric authentication functionality utilizing facial recognition is selected, the personal digital assistant captures the user's facial features.

[0101] If the password based authentication functionality is selected, the personal digital assistant captures the user password input.

[0102] If the cryptographic key based authentication functionality selected, the personal digital assistant employs a cryptographic key typically stored in its memory.

[0103] In all of the foregoing cases, the personal digital assistant communicates authentication information to the authenticator using the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0104] If the Bluetooth authentication functionality is selected, the personal digital assistant carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the personal digital assistant requests that the Bluetooth hub send an authentication confirmation to the authenticator. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0105] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the personal digital assistant and the authenticator negotiate the next authentication functionality and proceed as described hereinabove. If no additional authentication functions are required, the authenticator transmits an authentication confirmation to the personal digital assistant.

[0106] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the personal digital assistant, which displays a suitable message to the user.

[0107] Fig. 10B illustrates two different authentication functionalities for a wireless smart card. As seen in Fig. 10B, a wireless smart card, here designated by reference numeral 1010, provides cryptographic authentication and communicates with

an authenticator 1011, typically at least partially using a Bluetooth communication protocol.

[0108] Additionally or alternatively, a wireless smart card, which may be of conventional design and construction, here designated by reference numeral 1012, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0109] It is appreciated that authentication may be provided in the embodiment of Fig. 10B by any one or more of the authentication devices and/or functionalities described hereinabove.

[0110] Reference is now made to Fig. 13B, which illustrates the authentication functionalities shown in Fig. 10B. As seen in Fig. 13B, a user who requests access to a resource protected by an authenticator may employ a wireless smart card to negotiate an authentication functionality. Depending on the facilities available in or in association with the wireless smart card, one of the following authentication functionalities may be selected:

cryptographic key based; and

Bluetooth based.

[0111] If the cryptographic key based authentication functionality selected, the wireless smart card employs a cryptographic key typically stored in its memory.

[0112] In this case, the wireless smart card communicates authentication information to the authenticator using the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0113] If the Bluetooth authentication functionality is selected, the wireless smart card carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the wireless smart card requests that the Bluetooth hub send an authentication confirmation to the authenticator. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0114] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the wireless smart card and the authenticator negotiate the next authentication functionality and proceed as described hereinabove. If

no additional authentication functions are required, the authenticator transmits an authentication confirmation to the wireless smart card.

[0115] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the wireless smart card, which communicates a suitable message to the user.

[0116] Fig. 10C illustrates five different authentication functionalities for a cellular phone. As seen in Fig. 10C, a cellular phone with associated camera, here designated by reference numeral 1020, provides authentication using facial recognition and communicates with an authenticator 1021, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0117] Additionally or alternatively, a cellular phone having suitable touch screen functionality and/or an associated camera or scanner here designated by reference numeral 1022, provides authentication using fingerprint recognition and/or facial recognition and communicates with authenticator 1021, typically at least partially using a Bluetooth communication protocol.

[0118] Additionally or alternatively, a cellular phone, which may be of conventional design and construction, here designated by reference numeral 1024, provides password based authentication and communicates with authenticator 1021, typically at least partially using a Bluetooth communication protocol.

[0119] Additionally or alternatively, a cellular phone, which may be of conventional design and construction, here designated by reference numeral 1026, provides cryptographic authentication and communicates with authenticator 1021, typically at least partially using a Bluetooth communication protocol.

[0120] Additionally or alternatively, a cellular phone, which may be of conventional design and construction, here designated by reference numeral 1028, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0121] It is appreciated that authentication may be provided in the embodiment of Fig. 10C by any one or more of the authentication devices and/or functionalities described hereinabove.

[0122] Reference is now made to Fig. 13C, which illustrates the authentication

functionalities shown in Fig. 10C. As seen in Fig. 13C, a user who requests access to a resource protected by an authenticator may employ a cellular phone to negotiate an authentication functionality. Depending on the facilities available in or in association with the cellular phone, one of the following authentication functionalities may be selected:

biometric utilizing fingerprint recognition;

biometric utilizing facial recognition;

password based;

cryptographic key based; and

Bluetooth based.

[0123] If the biometric authentication functionality utilizing fingerprint recognition is selected, the cellular phone captures the user's fingerprint data.

[0124] If the biometric authentication functionality utilizing facial recognition is selected, the cellular phone captures the user's facial features.

[0125] If the password based authentication functionality is selected, the cellular phone captures the user password input.

[0126] If the cryptographic key based authentication functionality selected, the cellular phone employs a cryptographic key typically stored in its memory.

[0127] In all of the foregoing cases, the cellular phone communicates authentication information to the authenticator using the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0128] If the Bluetooth authentication functionality is selected, the cellular phone carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the cellular phone requests that the Bluetooth hub send an authentication confirmation to the authenticator. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0129] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the cellular phone and the authenticator negotiate the next authentication functionality and proceed as described hereinabove. If

no additional authentication functions are required, the authenticator transmits an authentication confirmation to the cellular phone.

[0130] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the cellular phone, which displays a suitable message to the user.

[0131] Fig. 10D illustrates two different authentication functionalities for an electronic wallet. As seen in Fig. 10D, an electronic wallet, here designated by reference numeral 1030, provides cryptographic authentication and communicates with an authenticator 1031, typically at least partially using a Bluetooth communication protocol.

[0132] Additionally or alternatively, an electronic wallet, which may be of conventional design and construction, here designated by reference numeral 1032, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0133] It is appreciated that authentication may be provided in the embodiment of Fig. 10D by any one or more of the authentication devices and/or functionalities described hereinabove.

[0134] Reference is now made to Fig. 13D, which illustrates the authentication functionalities shown in Fig. 10D. As seen in Fig. 13D, a user who requests access to a resource protected by an authenticator may employ an electronic wallet to negotiate an authentication functionality. Depending on the facilities available in or in association with the electronic wallet, one of the following authentication functionalities may be selected:

cryptographic key based; and

Bluetooth based.

[0135] If the cryptographic key based authentication functionality selected, the electronic wallet employs a cryptographic key typically stored in its memory.

[0136] In this case, the electronic wallet communicates authentication information to the authenticator using the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0137] If the Bluetooth authentication functionality is selected, the electronic

wallet carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the electronic wallet requests that the Bluetooth hub send an authentication confirmation to the authenticator. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0138] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the electronic wallet and the authenticator negotiate the next authentication functionality and proceed as described hereinabove. If no additional authentication functions are required, the authenticator transmits an authentication confirmation to the electronic wallet.

[0139] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the electronic wallet, which communicates a suitable message to the user.

[0140] Fig. 10E illustrates eight different authentication functionalities for a PC. As seen in Fig. 10E, a PC with associated camera, here designated by reference numeral 1040, provides authentication using facial recognition and communicates with an authenticator 1041, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0141] Additionally or alternatively, a PC having suitable touch screen functionality and/or an associated camera or scanner here designated by reference numeral 1042, provides authentication using fingerprint recognition and communicates with authenticator 1041, typically at least partially using a Bluetooth communication protocol.

[0142] Additionally or alternatively, a PC, which may be of conventional design and construction, here designated by reference numeral 1043, provides password based authentication and communicates with authenticator 1041, typically at least partially using a Bluetooth communication protocol.

[0143] Additionally or alternatively, a PC which may be of conventional design and construction, here designated by reference numeral 1044, provides cryptographic authentication and communicates with authenticator 1041, typically employing a

memory based key, typically at least partially using a Bluetooth communication protocol.

[0144] Additionally or alternatively, a PC with an associated suitable USB token, here designated by reference numeral 1045, provides cryptographic authentication and communicates with authenticator 1041, typically at least partially using a Bluetooth communication protocol.

[0145] Additionally or alternatively, a PC with associated smart card, here designated by reference numeral 1047, provides cryptographic authentication and communicates with authenticator 1041, typically at least partially using a Bluetooth communication protocol.

[0146] Additionally or alternatively, a PC with an associated suitable key diskette, here designated by reference numeral 1046, provides cryptographic authentication and communicates with authenticator 1041, typically at least partially using a Bluetooth communication protocol.

[0147] Additionally or alternatively, a PC, which may be of conventional design and construction, here designated by reference numeral 1048, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0148] It is appreciated that authentication may be provided in the embodiment of Fig. 10E by any one or more of the authentication devices and/or functionalities described hereinabove.

[0149] Reference is now made to Fig. 13E, which illustrates the authentication functionalities shown in Fig. 10E. As seen in Fig. 13E, a user who requests access to a resource protected by an authenticator may employ a PC to negotiate an authentication functionality. Depending on the facilities available in or in association with the PC, one of the following authentication functionalities may be selected:

biometric utilizing fingerprint recognition;

biometric utilizing facial recognition;

password based;

cryptographic utilizing a memory based key;

cryptographic utilizing a USB token based key;

cryptographic utilizing a smart card based key;

cryptographic utilizing a diskette based key; and

Bluetooth based.

[0150] If the biometric authentication functionality utilizing fingerprint recognition is selected, the PC captures the user's fingerprint data.

[0151] If the biometric authentication functionality utilizing facial recognition is selected, the PC captures the user's facial features.

[0152] If the password based authentication functionality is selected, the PC captures the user password input.

[0153] If the cryptographic memory based key authentication functionality is selected, the PC employs a cryptographic key typically stored in its memory.

[0154] If the cryptographic USB token based key authentication functionality is selected, the PC employs a cryptographic key typically stored in the associated USB key.

[0155] If the cryptographic smart card based key authentication functionality is selected, the PC employs a cryptographic key typically stored in the associated smart card.

[0156] If the cryptographic diskette based key authentication functionality is selected, the PC employs a cryptographic key typically stored in the associated key diskette.

[0157] In all of the foregoing cases, the PC communicates authentication information to the authenticator using the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0158] If the Bluetooth authentication functionality is selected, the PC carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the PC requests that the Bluetooth hub send an authentication confirmation to the authenticator. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0159] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the PC and the authenticator negotiate the next authentication functionality and proceed as described hereinabove. If no additional

authentication functions are required, the authenticator transmits an authentication confirmation to the PC.

[0160] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the PC, which displays a suitable message to the user.

[0161] Reference is now made to Figs. 11A, 11B, 11C, 11D, 11E and 11F which are simplified pictorial illustrations of combinations of authentication functionalities appropriate for six different combinations of different types of authentication devices and to Figs. 14A, 14B, 14C, 14D, 14E and 14F, which are simplified flow charts of combinations of authentication functionalities appropriate for six different types of authentication devices and correspond to Figs. 11A - 11F.

[0162] Fig. 11A illustrates two different authentication functionalities for a wireless smart card, here designated by reference numeral 1100 and three different authentication functionalities for a PC with associated camera or scanner, here designated by reference numeral 1102. The five different functionalities may be combined in any combination of two or more functionalities to provide authentication in conjunction with an authenticator 1103, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0163] As seen in Fig. 11A, wireless smart card 1100 provides cryptographic authentication functionality and communicates with authenticator 1103, typically at least partially using a Bluetooth communication protocol.

[0164] Additionally or alternatively, wireless smart card 1100 provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0165] Additionally or alternatively, the PC having an associated camera or scanner 1102, provides biometric authentication functionality using typically one or both of facial recognition and fingerprint recognition and communicates with authenticator 1103, typically at least partially using a Bluetooth communication protocol.

[0166] Additionally or alternatively, the PC 1102 provides password based authentication functionality and communicates with authenticator 1103, typically at least partially using a Bluetooth communication protocol.

[0167] It is appreciated that authentication may be provided in the embodiment of Fig. 11A by any one or more of the authentication devices and/or functionalities described hereinabove.

[0168] Reference is now made to Fig. 14A, which illustrates the authentication functionalities shown in Fig. 11A. As seen in Fig. 14A, a user employs the functionalities of Figs. 13B and 13E typically in series in order to provide authentication. The user preferably negotiates with an authenticator to determine whether the functionality of Fig. 13B is employed prior to that of Fig. 13E or vice versa.

[0169] Fig. 11B illustrates three different authentication functionalities for a cellular phone with associated camera, here designated by reference numeral 1110 and four different authentication functionalities for a PC with associated camera or scanner, here designated by reference numeral 1112. The seven different functionalities may be combined in any combination of two or more functionalities to provide authentication in conjunction with an authenticator 1113, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0170] As seen in Fig. 11B, cellular phone with associated camera 1110 provides biometric authentication functionality utilizing facial recognition and communicates with authenticator 1113, typically at least partially using a Bluetooth communication protocol.

[0171] Additionally or alternatively cellular phone 1110, which may be of conventional design and construction, provides password based authentication functionality and communicates with authenticator 1113, typically at least partially using a Bluetooth communication protocol.

[0172] Additionally or alternatively cellular phone 1110, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0173] Additionally or alternatively, the PC having an associated camera or scanner 1112 provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator 1113, typically at least partially using a Bluetooth communication protocol.

[0174] Additionally or alternatively, the PC 1112 provides password based authentication functionality and communicates with authenticator 1113, typically at

least partially using a Bluetooth communication protocol.

[0175] Additionally or alternatively, the PC 1112 provides cryptographic authentication functionality utilizing a diskette based key and communicates with authenticator 1113, typically at least partially using a Bluetooth communication protocol.

[0176] Additionally or alternatively, the PC 1112 provides cryptographic authentication functionality utilizing USB token based key and communicates with authenticator 1113, typically at least partially using a Bluetooth communication protocol.

[0177] It is appreciated that authentication may be provided in the embodiment of Fig. 11B by any one or more of the authentication devices and/or functionalities described hereinabove.

[0178] Reference is now made to Fig. 14B, which illustrates the authentication functionalities shown in Fig. 11B. As seen in Fig. 14B, a user employs the functionalities of Figs. 13C and 13E typically in series in order to provide authentication. The user preferably negotiates with an authenticator to determine whether the functionality of Fig. 13C is employed prior to that of Fig. 13E or vice versa.

[0179] Fig. 11C illustrates four different authentication functionalities for a personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner, here designated by reference numeral 1120 and four different authentication functionalities for a PC with associated camera or scanner, here designated by reference numeral 1122. The eight different functionalities may be combined in any combination of two or more functionalities to provide authentication in conjunction with an authenticator 1123, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.**[0110]**

[0180] As seen in Fig. 11C, personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner 1120 provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator 1123, typically at least partially using a Bluetooth communication protocol.

[0181] Additionally or alternatively personal digital assistant 1120, which may be of conventional design and construction, provides password based authentication

functionality and communicates with authenticator 1123, typically at least partially using a Bluetooth communication protocol.

[0182] Additionally or alternatively personal digital assistant 1120, which may be of conventional design and construction, provides cryptographic authentication functionality and communicates with authenticator 1123, typically at least partially using a Bluetooth communication protocol.

[0183] Additionally or alternatively personal digital assistant 1120, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0184] Additionally or alternatively, a PC having an associated camera or scanner 1122, provides biometric authentication functionality using typically fingerprint recognition and communicates with authenticator 1123, typically at least partially using a Bluetooth communication protocol.

[0185] Additionally or alternatively, the PC 1122, which may be of conventional design and manufacturing, provides password based authentication functionality and communicates with authenticator 1123, typically at least partially using a Bluetooth communication protocol.

[0186] Additionally or alternatively, the PC 1122 with associated smart card provides cryptographic authentication functionality utilizing smart card based key and communicates with authenticator 1123, typically at least partially using a Bluetooth communication protocol.

[0187] Additionally or alternatively, the PC 1122, which may be of conventional design and manufacturing, provides cryptographic authentication functionality utilizing memory based key authentication and communicates with authenticator 1123, typically at least partially using a Bluetooth communication protocol.

[0188] It is appreciated that authentication may be provided in the embodiment of Fig. 11C by any one or more of the authentication devices and/or functionalities described hereinabove.

[0189] Reference is now made to Fig. 14C, which illustrates the authentication functionalities shown in Fig. 11C. As seen in Fig. 14C, a user employs the functionalities of Figs. 13A and 13E typically in series in order to provide

authentication. The user preferably negotiates with an authenticator to determine whether the functionality of Fig. 13A is employed prior to that of Fig. 13E or vice versa.

[0190] Fig. 11D illustrates four different authentication functionalities for a personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner, here designated by reference numeral 1130 and three different authentication functionalities for a cellular phone with associated camera or scanner, here designated by reference numeral 1132. The seven different functionalities may be combined in any combination of two or more functionalities to provide authentication in conjunction with an authenticator 1133, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0191] As seen in Fig. 11D, personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner 1130 provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator 1133, typically at least partially using a Bluetooth communication protocol.

[0192] Additionally or alternatively personal digital assistant 1130, which may be of conventional design and construction, provides password based authentication functionality and communicates with authenticator 1133, typically at least partially using a Bluetooth communication protocol.

[0193] Additionally or alternatively personal digital assistant 1130, which may be of conventional design and construction, provides cryptographic authentication functionality and communicates with authenticator 1133, typically at least partially using a Bluetooth communication protocol.

[0194] Additionally or alternatively personal digital assistant 1130, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0195] Additionally or alternatively, a cellular phone having an associated camera or scanner 1132 provides biometric authentication functionality using typically facial recognition and communicates with authenticator 1133, typically at least partially using a Bluetooth communication protocol.

[0196] Additionally or alternatively, the cellular phone 1132, which may be of conventional design and manufacturing, provides password based authentication

functionality and communicates with authenticator 1133, typically at least partially using a Bluetooth communication protocol.

[0197] Additionally or alternatively cellular phone 1132, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0198] It is appreciated that authentication may be provided in the embodiment of Fig. 11D by any one or more of the authentication devices and/or functionalities described hereinabove.

[0199] Reference is now made to Fig. 14D, which illustrates the authentication functionalities shown in Fig. 11D. As seen in Fig. 14D, a user employs the functionalities of Figs. 13A and 13C typically in series in order to provide authentication. The user preferably negotiates with an authenticator to determine whether the functionality of Fig. 13A is employed prior to that of Fig. 13C or vice versa.

[0200] Fig. 11E illustrates three different authentication functionalities for a personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner, here designated by reference numeral 1140 and two different authentication functionalities for a wireless smart card, here designated by reference numeral 1142. The five different functionalities may be combined in any combination of two or more functionalities to provide authentication in conjunction with an authenticator 1143, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0201] As seen in Fig. 11E, personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner 1140 provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator 1143, typically at least partially using a Bluetooth communication protocol.

[0202] Additionally or alternatively personal digital assistant 1140, which may be of conventional design and construction, provides password based authentication functionality and communicates with authenticator 1143, typically at least partially using a Bluetooth communication protocol.

[0203] Additionally or alternatively personal digital assistant 1140, which may

be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0204] Additionally or alternatively wireless smart card 1142 provides cryptographic authentication functionality and communicates with authenticator 1143, typically at least partially using a Bluetooth communication protocol.

[0205] Additionally or alternatively wireless smart card 1142, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0206] It is appreciated that authentication may be provided in the embodiment of Fig. 11E by any one or more of the authentication devices and/or functionalities described hereinabove.

[0207] Reference is now made to Fig. 14E, which illustrates the authentication functionalities shown in Fig. 11E. As seen in Fig. 14E, a user employs the functionalities of Figs. 13A and 13B typically in series in order to provide authentication. The user preferably negotiates with an authenticator to determine whether the functionality of Fig. 13A is employed prior to that of Fig. 13B or vice versa.

[0208] Fig. 11F illustrates two different authentication functionalities for an electronic wallet, here designated by reference numeral 1150 and four different authentication functionalities for a cellular phone having an associated camera or scanner, here designated by reference numeral 1152. The five different functionalities may be combined in any combination of two or more functionalities to provide authentication in conjunction with an authenticator 1153, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0209] As seen in Fig. 11F, wireless smart card 1152 provides cryptographic authentication functionality and communicates with authenticator 1153, typically at least partially using a Bluetooth communication protocol.

[0210] Additionally or alternatively wireless smart card 1152, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0211] Additionally or alternatively cellular phone having an associated camera or scanner 1152 provides biometric authentication functionality employing typically

facial and/or fingerprint recognition and communicates with authenticator 1153, typically at least partially using a Bluetooth communication protocol.

[0212] Additionally or alternatively cellular phone 1152, which may be of conventional design and manufacturing, provides password based authentication functionality and communicates with authenticator 1153, typically at least partially using a Bluetooth communication protocol.

[0213] Additionally or alternatively cellular phone 1152, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0214] It is appreciated that authentication may be provided in the embodiment of Fig. 11F by any one or more of the authentication devices and/or functionalities described hereinabove.

[0215] Reference is now made to Fig. 14F, which illustrates the authentication functionalities shown in Fig. 11F. As seen in Fig. 14F, a user employs the functionalities of Figs. 13C and 13D typically in series in order to provide authentication. The user preferably negotiates with an authenticator to determine whether the functionality of Fig. 13C is employed prior to that of Fig. 13D or vice versa.

[0216] Reference is now made to Figs. 12A, 12B and 12C, which are simplified pictorial illustrations of combinations of authentication functionalities appropriate for three different types of multi-tier authentication systems.

[0217] Fig. 12A illustrates four different authentication functionalities for a PC with associated camera or scanner, here designated by reference numeral 1200, four different authentication functionalities for a personal digital assistant with suitable touch screen functionality and/or an associated camera or scanner, here designated by reference numeral 1202 and two different authentication functionalities for a wireless smart card, here designated by reference numeral 1204. The ten different functionalities may be combined in any combination of two or more functionalities to provide multi-tier authentication in conjunction with an authenticator 1205, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0218] As seen in Fig. 12A a PC having an associated camera or scanner 1200, provides biometric authentication functionality using typically fingerprint recognition

and communicates with authenticator 1205, typically at least partially using a Bluetooth communication protocol.

[0219] Additionally or alternatively, the PC 1200, which may be of conventional design and manufacturing, provides password based authentication functionality and communicates with authenticator 1205, typically at least partially using a Bluetooth communication protocol.

[0220] Additionally or alternatively, the PC 1200 with associated USB token provides cryptographic authentication functionality utilizing USB token based key and communicates with authenticator 1205, typically at least partially using a Bluetooth communication protocol.

[0221] Additionally or alternatively, the PC 1200, which may be of conventional design and manufacturing, provides cryptographic authentication functionality utilizing memory based key authentication and communicates with authenticator 1205, typically at least partially using a Bluetooth communication protocol.

[0222] Additionally or alternatively, personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner 1202 provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator 1205, typically at least partially using a Bluetooth communication protocol.

[0223] Additionally or alternatively personal digital assistant 1202, which may be of conventional design and construction, provides password based authentication functionality and communicates with authenticator 1205, typically at least partially using a Bluetooth communication protocol.

[0224] Additionally or alternatively personal digital assistant 1202, which may be of conventional design and construction, provides cryptographic authentication functionality and communicates with authenticator 1205, typically at least partially using a Bluetooth communication protocol.

[0225] Additionally or alternatively personal digital assistant 1202, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0226] Additionally or alternatively wireless smart card 1204 provides

cryptographic authentication functionality and communicates with authenticator 1205, typically at least partially using a Bluetooth communication protocol.

[0227] Additionally or alternatively, wireless smart card 1204 provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0228] It is appreciated that multi-tier authentication may be provided in the embodiment of Fig. 12A by any one or more combinations of the authentication devices and/or functionalities described hereinabove.

[0229] Fig. 12B illustrates four different authentication functionalities for a personal digital assistant with suitable touch screen functionality and/or associated camera or scanner, here designated by reference numeral 1210, four different authentication functionalities for a cellular phone with an associated camera or scanner, here designated by reference numeral 1212 and two different authentication functionalities for an electronic wallet, here designated by reference numeral 1214. The ten different functionalities may be combined in any combination of two or more functionalities to provide multi-tier authentication in conjunction with an authenticator 1215, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0230] As seen in Fig. 12B personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner 1210 provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator 1215, typically at least partially using a Bluetooth communication protocol.

[0231] Additionally or alternatively personal digital assistant 1210, which may be of conventional design and construction, provides password based authentication functionality and communicates with authenticator 1215, typically at least partially using a Bluetooth communication protocol.

[0232] Additionally or alternatively personal digital assistant 1210, which may be of conventional design and construction, provides cryptographic authentication functionality and communicates with authenticator 1215, typically at least partially using a Bluetooth communication protocol.

[0233] Additionally or alternatively personal digital assistant 1210, which may

be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0234] Additionally or alternatively cellular phone with associated camera, here designated by reference numeral 1212, provides authentication using facial recognition and communicates with an authenticator 1215, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0235] Additionally or alternatively, a cellular phone, which may be of conventional design and construction, here designated by reference numeral 1212, provides password based authentication and communicates with authenticator 1215, typically at least partially using a Bluetooth communication protocol.

[0236] Additionally or alternatively, cellular phone, which may be of conventional design and construction, here designated by reference numeral 1212, provides cryptographic authentication and communicates with authenticator 1215, typically at least partially using a Bluetooth communication protocol.

[0237] Additionally or alternatively, cellular phone, which may be of conventional design and construction, here designated by reference numeral 1212, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0238] Additionally or alternatively, electronic wallet, here designated by reference numeral 1214, provides cryptographic authentication and communicates with an authenticator 1215, typically at least partially using a Bluetooth communication protocol.

[0239] Additionally or alternatively, electronic wallet, which may be of conventional design and construction, here designated by reference numeral 1214, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0240] It is appreciated that multi-tier authentication may be provided in the embodiment of Fig. 12B by any one or more combinations of the authentication devices and/or functionalities described hereinabove.

[0241] Fig. 12C illustrates four different authentication functionalities for a cellular phone with suitable touch screen functionality and/or associated camera or scanner, here designated by reference numeral 1220, four different authentication

functionalities for a personal digital assistant with a suitable touch screen and/or an associated camera or scanner, here designated by reference numeral 1222, four different authentication functionalities for a PC with a suitable touch screen and an associated camera or scanner, here designated by reference numeral 1224, and two different authentication functionalities for a wireless smart card, here designated by reference numeral 1226. The fourteen different functionalities may be combined in any combination of two or more functionalities to provide multi-tier authentication in conjunction with an authenticator 1227, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0242] As seen in Fig. 12C cellular phone with associated camera, here designated by reference numeral 1220, provides authentication using facial recognition and communicates with an authenticator 1227, designated by a lock symbol, typically at least partially using a Bluetooth communication protocol.

[0243] Additionally or alternatively, a cellular phone, which may be of conventional design and construction, here designated by reference numeral 1220, provides password based authentication and communicates with authenticator 1227, typically at least partially using a Bluetooth communication protocol.

[0244] Additionally or alternatively, cellular phone, which may be of conventional design and construction, here designated by reference numeral 1220, provides cryptographic authentication and communicates with authenticator 1227, typically at least partially using a Bluetooth communication protocol.

[0245] Additionally or alternatively, cellular phone, which may be of conventional design and construction, here designated by reference numeral 1220, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0246] Additionally or alternatively, personal digital assistant having suitable touch screen functionality and/or an associated camera or scanner 1222 provides biometric authentication functionality utilizing fingerprint recognition and communicates with authenticator 1227, typically at least partially using a Bluetooth communication protocol.

[0247] Additionally or alternatively personal digital assistant 1222, which may be of conventional design and construction, provides password based authentication

functionality and communicates with authenticator 1227, typically at least partially using a Bluetooth communication protocol.

[0248] Additionally or alternatively personal digital assistant 1222, which may be of conventional design and construction, provides cryptographic authentication functionality and communicates with authenticator 1227, typically at least partially using a Bluetooth communication protocol.

[0249] Additionally or alternatively personal digital assistant 1222, which may be of conventional design and construction, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0250] Additionally or alternatively the PC having an associated camera or scanner 1224, provides biometric authentication functionality using typically fingerprint recognition and communicates with authenticator 1227, typically at least partially using a Bluetooth communication protocol.

[0251] Additionally or alternatively, PC 1224, which may be of conventional design and manufacturing, provides password based authentication functionality and communicates with authenticator 1227, typically at least partially using a Bluetooth communication protocol.

[0252] Additionally or alternatively, PC 1224, which may be of conventional design and manufacturing, provides cryptographic authentication functionality utilizing suitable key diskette authentication and communicates with authenticator 1227, typically at least partially using a Bluetooth communication protocol.

[0253] Additionally or alternatively, PC 1224, which may be of conventional design and manufacturing, provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0254] Additionally or alternatively wireless smart card 1226 provides cryptographic authentication functionality and communicates with authenticator 1227, typically at least partially using a Bluetooth communication protocol.

[0255] Additionally or alternatively, wireless smart card 1226 provides authentication employing authentication functionality, which forms part of a Bluetooth communication protocol.

[0256] It is appreciated that multi-tier authentication may be provided in the embodiment of Fig. 12C by any one or more combinations of the authentication devices

and/or functionalities described hereinabove.

[0257] Reference is now made to Figs. 15A, 15B, 15C, 15D and 15E, which are simplified flow charts of methods for obtaining authentication information for five different types of authentication devices.

[0258] Fig. 15A illustrates methods for obtaining authentication information suitable for a personal digital assistant. As seen in Fig. 15A depending on the facilities available in or in association with the personal digital assistant, one of the following authentication functionalities which require obtaining authentication information may be selected:

biometric utilizing fingerprint recognition;

biometric utilizing facial recognition;

password based; and

cryptographic key based.

[0259] If the biometric authentication functionality utilizing fingerprint recognition is selected, the personal digital assistant captures the user's fingerprint data.

[0260] If the biometric authentication functionality utilizing facial recognition is selected, the personal digital assistant captures the user's facial features.

[0261] If the password based authentication functionality is selected, the personal digital assistant captures the user password input.

[0262] If the cryptographic key based authentication functionality selected, the personal digital assistant employs a cryptographic key typically stored in its memory.

[0263] Fig. 15B illustrates methods for obtaining authentication information suitable for a wireless smart card. As seen in Fig. 15B depending on the facilities available in or in association with the wireless smart card, one of the following authentication functionalities which require obtaining authentication information may be selected:

cryptographic key based.

If the cryptographic key based authentication functionality selected, the wireless smart card employs a cryptographic key typically stored in its memory.

[0264] Fig. 15C illustrates methods for obtaining authentication information suitable for a cellular phone. As seen in Fig. 15C depending on the facilities available in or in association with the cellular phone, one of the following authentication

functionalities which require obtaining authentication information may be selected:

biometric utilizing fingerprint recognition;

biometric utilizing facial recognition;

password based; and

cryptographic key based.

[0265] If the biometric authentication functionality utilizing fingerprint recognition is selected, the cellular phone captures the user's fingerprint data.

[0266] If the biometric authentication functionality utilizing facial recognition is selected, the cellular phone captures the user's facial features.

[0267] If the password based authentication functionality is selected, the cellular phone captures the user password input.

[0268] If the cryptographic key based authentication functionality selected, the cellular phone employs a cryptographic key typically stored in its memory.

[0269] Fig. 15D illustrates methods for obtaining authentication information suitable for an electronic wallet. As seen in Fig. 15D depending on the facilities available in or in association with the electronic wallet, one of the following authentication functionalities which require obtaining authentication information may be selected:

cryptographic key based.

If the cryptographic key based authentication functionality selected, the electronic wallet employs a cryptographic key typically stored in its memory.

[0270] Fig. 15E illustrates methods for obtaining authentication information suitable for a PC. As seen in Fig. 15E depending on the facilities available in or in association with the PC, one of the following authentication functionalities which require obtaining authentication information may be selected:

biometric utilizing fingerprint recognition;

biometric utilizing facial recognition;

password based;

cryptographic utilizing a memory based key;

cryptographic utilizing a USB token based key;

cryptographic utilizing a smart card based key; and

cryptographic utilizing a diskette based key.

[0271] If the biometric authentication functionality utilizing fingerprint recognition is selected, the PC captures the user's fingerprint data.

[0272] If the biometric authentication functionality utilizing facial recognition is selected, the PC captures the user's facial features.

[0273] If the password based authentication functionality is selected, the PC captures the user password input.

[0274] If the cryptographic memory based key authentication functionality is selected, the PC employs a cryptographic key typically stored in its memory.

[0275] If the cryptographic USB token based key authentication functionality is selected, the PC employs a cryptographic key typically stored in the associated USB key.

[0276] If the cryptographic smart card based key authentication functionality is selected, the PC employs a cryptographic key typically stored in the associated smart card.

[0277] If the cryptographic diskette based key authentication functionality is selected, the PC employs a cryptographic key typically stored in the associated key diskette.

[0278] Reference is now made to Figs. 16A, 16B and 16C, which are simplified flow charts of different multi-tier and non multi-tier authentication using different communication modes between an authenticating device and an authenticator.

[0279] Fig. 16A illustrates a non multi-tier authentication using a direct communication mode between an authenticating device and an authenticator. As seen in Fig. 16A, an authentication device such as a personal digital assistant, a wireless smart card, a cellular phone, an electronic wallet or a PC negotiates with an authenticator an authentication functionality. Depending on the facilities available in or in association with the authentication device, either a Bluetooth based authentication functionality or non-Bluetooth based authentication functionality may be used.

[0280] If a non-Bluetooth authentication is selected, the authentication device obtains authentication information employing at least one of the functionalities of Figs. 15A – 15E. The authentication device than communicates authentication information to the authenticator using at least partially the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0281] If the Bluetooth authentication functionality is selected, the authentication device carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the authentication device requests that the Bluetooth hub send an authentication confirmation to the authenticator. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0282] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the authentication device and the authenticator negotiate the next authentication functionality and proceed as described hereinabove. If no additional authentication functions are required, the authenticator transmits an authentication confirmation to the authentication device.

[0283] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the authentication device.

[0284] Fig. 16B illustrates a multi-tier authentication in which an authentication device and an authenticator employ a second device for communication. As seen in Fig. 16B an authentication device such as a personal digital assistant, a wireless smart card, a cellular phone, an electronic wallet or a PC negotiates with an authenticator an authentication functionality communicating through said second device, which may be a personal digital assistant, a cellular phone or a PC. Depending on the facilities available in or in association with the authentication device, either a Bluetooth based authentication functionality or non-Bluetooth based authentication functionality may be used.

[0285] If a non-Bluetooth authentication is selected, the authentication device obtains authentication information employing at least one of the functionalities of Figs. 15A – 15E. The authentication device than communicates authentication information to the authenticator using at least partially the Bluetooth communication protocol and communicating through said second device. In response to receipt of such information, the authenticator may authenticate the user.

[0286] If the Bluetooth authentication functionality is selected, the authentication device carries out Bluetooth authentication in conjunction with a

Bluetooth hub. If the authentication is successful, the authentication device requests that the Bluetooth hub send an authentication confirmation to the authenticator communicating through said second device. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0287] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the authentication device and the authenticator negotiate the next authentication functionality communicating through said second device and proceed as described hereinabove. If no additional authentication functions are required, the authenticator transmits an authentication confirmation to the authentication device communicating through said second device.

[0288] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the authentication device communicating through said second device.

[0289] Fig. 16C illustrates a multi-tier authentication in which an authentication device employ a proxy to communicate with an authenticator. As seen in Fig. 16C an authentication device such as a personal digital assistant, a wireless smart card, a cellular phone, an electronic wallet or a PC negotiates with an authenticator an authentication functionality, said negotiation employing a proxy, which may be a personal digital assistant, a cellular phone or a PC, to communicate with the authenticator. Depending on the facilities available in or in association with the authentication device, either a Bluetooth based authentication functionality or non-Bluetooth based authentication functionality may be used.

[0290] If a non-Bluetooth authentication is selected, the authentication device obtains authentication information employing at least one of the functionalities of Figs. 15A – 15E. The authentication device transmits authentication information to the proxy. The proxy then transmits the data to the authenticator. One or more of the transmissions use at least partially the Bluetooth communication protocol. In response to receipt of such information, the authenticator may authenticate the user.

[0291] If the Bluetooth authentication functionality is selected, the

authentication device carries out Bluetooth authentication in conjunction with a Bluetooth hub. If the authentication is successful, the authentication device requests that the Bluetooth hub send an authentication confirmation to the proxy. The proxy then sends the confirmation to the authenticator. In response to receipt of the confirmation, the authenticator determines whether the hub, which sent the confirmation, is certified to do so.

[0292] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication functions are required. If so, the authentication device and the authenticator negotiate the next authentication functionality, said negotiation employing a proxy, and proceed as described hereinabove. If no additional authentication functions are required, the authenticator transmits an authentication confirmation to the proxy. The proxy then transmits the confirmation to the authentication device.

[0293] If authentication of the user and/or device is not successful at any stage, indicating that the user and/or device is not authorized, the authenticator transmits a non-authentication message to the proxy. The proxy then transmits the non-authentication message to the authentication device.

[0294] Reference is now made to Figs. 17A, 17B and 17C, which are simplified flow charts of different multi-tier and non multi-tier authentication employing different combinations of authentication devices.

[0295] Fig. 17A illustrates a non multi-tier authentication employing a single authentication device. As seen in Fig. 17A, a user who requests access to a resource protected by an authenticator may employ an authentication device. The authentication device may employ any one of the functionalities of Figs. 16A – 16C to perform authentication with the authenticator. When the authentication device receives a confirmation message or a non-authentication message, the authentication device displays a suitable message to the user.

[0296] Fig. 17B illustrates a non multi-tier authentication employing multiple authentication devices. As seen in Fig. 17B, a user who requests access to a resource protected by an authenticator negotiates with said authenticator an authentication device. The authentication device may employ any one of the functionalities of Figs. 16A – 16C to perform authentication with the authenticator.

[0297] If authentication of the user and/or device is successful, indicating that the user and/or device is authorized, a determination is made as to whether additional authentication devices are required. If so, the user and the authenticator negotiate the next authentication device and proceed as described hereinabove. If no additional authentication devices are required, an authentication is granted.

[0298] If authentication of the user and/or device is not successful at any stage, authentication is not granted.

[0299] Fig. 17C illustrates a multi-tier authentication employing an enabling device. As seen in Fig. 17C, a user who requests access to a resource protected by an authenticator may employ an authentication device. The authenticator may require the authentication device to be enabled for authentication by an enabling device. The enabling device may employ any one of the functionalities of Figs. 16A – 16C to perform authentication with the authenticator.

[0300] If the enabling device is successfully authenticated, the authentication device may employ any one of the functionalities of Figs. 16A – 16C to perform authentication with the authenticator. When the authentication device receives a confirmation message or a non-authentication message, the authentication device displays a suitable message to the user.

[0301] It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention includes both combinations and subcombinations of the various features described hereinabove as well as variations and modifications which would occur to persons skilled in the art upon reading the specification and which are not in the prior art.